



A new method for constructing designs and codes from the conjugacy classes of groups

Amin Saeidi¹ · Hadiseh Saydi² · Thekiso Seretlo²

Received: 3 November 2024 / Revised: 16 April 2025 / Accepted: 16 September 2025

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2025

Abstract

In this paper, we present a novel method for constructing designs and codes from the conjugacy classes and subgroups of finite groups. The resulting designs are point- and block-transitive and invariant under the group action. We apply our method to the sporadic simple group J_1 (Janko group) and its maximal subgroups, as well as to the group $PSL_2(q)$, where q is a power of 2. Our method generalises the ‘Key–Moori Method 2’ and uncovers several designs and codes not captured by that approach. Notably, it is effective for both maximal and non-maximal subgroups, broadening the scope of design construction. In particular, we provide specific examples of designs derived from non-maximal subgroups of $PSL_2(q)$.

Keywords Conjugacy classes · Designs · The Projective linear group · The Janko group

Mathematics Subject Classification 05B05 · 20D05 · 94B05

1 Introduction

The structure of a group is deeply connected to the structure of the objects it preserves. In [8], J. D. Key and J. Moorí developed two methods to construct designs from a maximal subgroup and conjugacy classes of a primitive group G and presented some results for the Janko groups J_1 and J_2 . Both these methods and some interesting examples have been summarised in [13].

The first method (Key–Moorí Method 1) deals with the construction of symmetric 1-designs and their corresponding codes obtained from the action of a simple group G on the

Hadiseh Saydi and Thekiso Seretlo have contributed equally to this work.

✉ Amin Saeidi
amin.saeidi@ul.ac.za

Hadiseh Saydi
hadisehsaydi90@gmail.com

Thekiso Seretlo
thekiso.seretlo@nwu.ac.za

¹ Department of Mathematics and Applied Mathematics, University of Limpopo, Polokwane, South Africa

² Pure and Applied Analytics, School of Mathematical and Statistical Sciences, North West University, Mahikeng Campus, Mmabatho, South Africa

cosets of a maximal subgroup. This method was applied to several sporadic simple groups [10, 17–20] and some families of finite simple groups [11, 12, 21–23]. The second method (Key–Moori Method 2) deals with the construction of 1-designs from a maximal subgroup of a primitive group G and its conjugacy classes. This method has also been applied to some families of finite simple groups and their conjugacy classes [12, 21, 22, 24].

In [14], J. Moori introduced a new method (Method 3) for constructing codes and designs from the fixed points of elements of finite transitive groups, and applied it to the sporadic simple groups HS and J_2 . The relationship between Key–Moori Method 2 and Method 3 have been studied in [27]. Method 3 was also applied to the fixed points of involutions of the alternating group A_n (for $n \geq 5$) [15] (see also [26]). Moreover, in [16], designs and codes were constructed from maximal pairwise commuting sets of 3-transpositions and as examples, the method was applied to symmetric groups and Fischer groups F_i for $i \in \{21, 22, 23, 24\}$. In this paper, we present a method that extends the Key–Moori Method 2 for constructing designs from conjugacy classes in a group G . Our approach allows for the construction of designs that Method 2 cannot capture. Furthermore, it enables the use of any subgroup $H \leq G$, not necessarily maximal, thereby broadening its applicability. Even in the case where G is a simple group and H is a maximal subgroup, our method provides a generalisation of Method 2, revealing new designs that were previously overlooked. We also note that in [4], a generalisation of Method 2 is presented. Our method, especially when applied to maximal subgroups, can be viewed as a special case of their framework (see Remark 1). However, our construction offers a practical approach to the explicit construction of designs. To illustrate this, we focus on new examples obtained via our method.

2 Terminology and notations

Our notation for designs and groups follows standard conventions, as outlined in [1] and ATLAS [3]. An incidence structure is represented by a triple $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{P}$ denotes the point set, $\mathcal{B}$ denotes the block set (disjoint from $\mathcal{P}$), and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ denotes the incidence set. If the ordered pair $(p, B) \in \mathcal{I}$, we say that p is incident with B . We can assume that the blocks in $\mathcal{B}$ are subsets of $\mathcal{P}$, so $(p, B) \in \mathcal{D}$ if and only if $p \in B$.

For a positive integer t , we say that $\mathcal{D}$ is a t -design if every block $B \in \mathcal{B}$ is incident with exactly k points, and every t distinct points are together incident with λ blocks. In this case, we write $\mathcal{D} = t-(v, k, \lambda)$, where $v = |\mathcal{P}|$ and $k = |B|$. The complement of $\mathcal{D}$ is the structure $\tilde{\mathcal{D}} = (\mathcal{P}, \tilde{\mathcal{B}}, \tilde{\mathcal{I}})$, where $\tilde{\mathcal{B}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$. The dual structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(B, p) \in \mathcal{I}^t$ if and only if $(p, B) \in \mathcal{I}$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$. We say that $\mathcal{D}$ is symmetric if it has the same number of points and blocks.

An isomorphism of two t -designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ and $\mathcal{D}' = (\mathcal{P}', \mathcal{B}')$ is a permutation of $\mathcal{P}$ which sends blocks of $\mathcal{D}$ to blocks of $\mathcal{D}'$. An isomorphism from $\mathcal{D}$ to itself is called an automorphism. The group of all automorphisms of $\mathcal{D}$ is denoted by $\text{Aut}(\mathcal{D})$.

A linear code C of length n and dimension k is an F_q -subspace of dimension k in the vector space F_q^n , where F_q is a field of q elements. We may write $C = [n, k]_q$. If $q = 2$ then we call C a binary code. Each element of C is a codeword. The Hamming distance of two distinct codewords c_1 and c_2 of a code C is the number of coordinate positions in which they differ. We denote the Hamming distance of c_1 and c_2 by $d(c_1, c_2)$. The smallest distance among all pairs of distinct codewords is called the minimum distance of C denoted by $d(C)$. The weight of a codeword c is defined to be $d(c, 0)$. We denote the weight of c by $\text{wt}(c)$. Note that the

linear property of $\mathcal{C}$ implies that there exists a codeword whose weight equals $d(\mathcal{C})$. Hence the minimum distance of a linear code is just the minimum weight of the code. Assume that $W = \{w_1, \dots, w_n\}$ is the set of weights of all codewords of $\mathcal{C}$, and $w_1 < \dots < w_n$. Then the weight distribution of $\mathcal{C}$ is defined as $w_1^{n_1} \dots w_k^{n_k}$, where n_i for each i is the number of codewords of weight w_i .

Let G be a finite group and let T be a non-empty subset of G . We define the normalizer of T as $N_G(T) = \{g \in G \mid T^g = T\}$. We also define $x^T = \{x^u \mid u \in T\}$. It is important to note that x need not be an element of T , so it is possible that $x^T \cap T = \emptyset$. This definition is a generalisation of the standard definition of x^H , for a subgroup H of G , which represents the conjugacy class of an element $x \in H$. We also define the centralizer of x in H as $C_H(x) = C_G(x) \cap H$. Again, notice that x need not be in H , so $C_H(x)$ might be a trivial subgroup of G .

Definition 1 Let G be a permutation group acting on a set Ω . For $g \in G$, let

$$\chi(g) = |\{\alpha \in \Omega \mid \alpha^g = \alpha\}|.$$

The non-negative integer valued function χ is called the permutation character associated with the action.

As it is well-known, a permutation character of G is in fact an ordinary character afforded by the permutation representation of G . In other words, if H is a point stabiliser of G , then $\chi_H = (\iota^G)_H$, where ι represents the trivial character of G . Moreover we have:

$$\chi_H(g) = \chi(G|\Omega)(g) = [N_G(H) : H]^{-1} \sum_{i=1}^m \frac{|C_G(g)|}{|C_H(h_i)|},$$

where h_i are representatives of the conjugacy classes of H that fuse to $[g] = C_g$ in G .

3 The method

In this section, we introduce a method for constructing 1-designs from arbitrary subgroups and conjugacy classes of G . In this approach, we treat the elements of the conjugacy class x^G as the points of the design, and for a subgroup H of G , the conjugates of the set x^H form the blocks. In a sense, this method can be viewed as a generalisation of Key–Moori Method 2. It not only produces the designs obtainable through Key–Moori Method 2 but also reveals a variety of additional designs.

Lemma 3.1 Let H be a subgroup of G , $x \in G$, and $T = x^H$. Then we have:

$$N_G(H) \cap C_G(x) \subseteq N_G(T) \subseteq C_G(x)H.$$

Proof For any element $g \in N_G(H) \cap C_G(x)$, we have $H^g = H$ and $x^g = x$. So, $x^{Hg} = x^{gH} = x^H$. Thus, $N_G(H) \cap C_G(x) \subseteq N_G(x^H)$. To prove the second inclusion, suppose that $g \in N_G(T)$. Hence for the identity element $1 \in H$, there exists an element $h \in H$ such that $x^{1g} = x^g = x^h$. Therefore, $gh^{-1} \in C_G(x)$ and $g \in C_G(x)H$. That is, $N_G(x^H) \subseteq C_G(x)H$ and the result follows. $\square$

Theorem 3.2 Let G be a finite group and H be a subgroup of G . For $x \in G$, let x^G be a conjugacy class of G , and let $\mathcal{B} = \{T^g \mid g \in G\}$, where $T = x^H$. If $T \neq \emptyset$, then we can construct a

$$1 - \left(|x^G|, |T|, \frac{|C_G(x):C_H(x)|}{|N_G(T):H|} \right)$$

design $\mathcal{D}(T)$. Moreover, G acts transitively on both points and blocks of $\mathcal{D}(T)$.

Proof We first prove that this structure is a 1-design. Assume that the element x belongs to exactly λ blocks, say $T^{y_1}, \dots, T^{y_\lambda}$. If y is an arbitrary element in x^G , then $y = x^g$ for some $g \in G$. Therefore, y belongs to $T^{y_1 g}, \dots, T^{y_\lambda g}$. As T^{y_i} s are distinct, so are $T^{y_i g}$ s. Therefore, we have constructed a $1-(|x^G|, |T|, \lambda)$ design. Notice that $v = |x^G|$ and $k = |T|$. Moreover, $b = |G:N_G(T)|$, the number of conjugates of T in G . Using the equation $\lambda = \frac{kb}{v}$, we can write:

$$\lambda = \frac{kb}{v} = \frac{|H|}{|C_H(x)|} \times \frac{|G|}{|N_G(T)|} \times \frac{|C_G(x)|}{|G|} = \frac{|C_G(x):C_H(x)|}{|N_G(T):H|}.$$

The transitivity of the action of G on both points and blocks is obvious. The proof is now completed. $\square$

Corollary 3.3 If H is a maximal subgroup of G and $x^H \neq \emptyset$, then we can construct a

$$1 - \left(|x^G|, |x^H|, \frac{|C_G(x)|}{|C_H(x)|} \right)$$

design.

Proof Since $H \leq N_G(T)$ and H is maximal, the result follows. $\square$

Definition 2 Let $\mathcal{D}_1$ be a $1-(v, k_1, \lambda_1)$ design and $\mathcal{D}_2$ be a $1-(v, k_2, \lambda_2)$ design. Suppose both 1-designs have the same point set $\mathcal{P}$ and disjoint block sets $\mathcal{B}_1$ and $\mathcal{B}_2$, i.e.

$$\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset.$$

Assume there exists a bijection $f: \mathcal{B}_1 \rightarrow \mathcal{B}_2$ such that for each block $B_1 \in \mathcal{B}_1$, we have $B_1 \cap f(B_1) = \emptyset$.

Define a new incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, where each block $B \in \mathcal{B}$ is of the form:

$$B = B_1 \cup f(B_1), \quad \text{for each } B_1 \in \mathcal{B}_1.$$

Denote this structure by $\mathcal{D}_1 \hat{\cup} \mathcal{D}_2$ and call it the merged design constructed from $\mathcal{D}_1$ and $\mathcal{D}_2$.

Lemma 3.4 Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be as defined in Definition 2. Then $\mathcal{D}_1 \hat{\cup} \mathcal{D}_2$ is a $1-(v, k_1 + k_2, \lambda_1 + \lambda_2)$ design.

Proof To show $\mathcal{D}$ that is a 1-design, we check each block in $\mathcal{D}$ has $k_1 + k_2$ points because each block B is formed by combining a block from $\mathcal{B}_1$ and its image under f . Additionally, every points is incident with $\lambda_1 + \lambda_2$ blocks in $\mathcal{D}$. Thus, $\mathcal{D}$ is a $1-(v, k_1 + k_2, \lambda_1 + \lambda_2)$ design. $\square$

Proposition 3.5 Let G be a finite group and H a subgroup of G . Suppose $\mathcal{D}_1$ and $\mathcal{D}_2$ are distinct designs constructed using the method outlined in Theorem 3.2. Then the merged design $\mathcal{D}_1 \hat{\cup} \mathcal{D}_2$ exists.

Proof Let x^H and y^H be representatives of blocks of $\mathcal{D}_1$ and $\mathcal{D}_2$, respectively. Define a function f by $f(x^{Hg}) = y^{Hg}$, where g is an element of G . It is straightforward to verify that this function f meets the requirements of Definition 2:

1. f is a bijection between $\mathcal{B}_1$ and $\mathcal{B}_2$.
2. For each block $B_1 \in \mathcal{B}_1$, the intersection $B_1 \cap f(B_1) = \emptyset$.

Therefore, the conditions in Definition 2 are satisfied, whence the merged design $\mathcal{D}_1 \hat{\cup} \mathcal{D}_2$ exists. $\square$

Remark 1 The construction method presented in Theorem 3.2 can be viewed as a special case of the general construction described in Theorem 3 of [4]. In their framework, a group G acts transitively on two sets Ω_1 and Ω_2 , with distinguished subsets $\Delta_1 \subseteq \Omega_1$ and $\Delta_2 \subseteq \Omega_2$. By taking $\Omega_1 = G$, $\Omega_2 = x^G$, $\Delta_1 = \{x\}$, and $\Delta_2 = x^H$ for some $x \in G$ and $H \leq G$, our case fits into their setup with $s = 1$ and $\delta_1 = x$. Furthermore, Proposition 3.5 corresponds to the case $s = 2$, $\delta_1 = x$, $\delta_2 = y$.

Proposition 3.6 Let H be a subgroup of a finite group G . For $x \in G$, let $\mathcal{D}(x)$ be a

$$1 - \left(|x^G|, |x^H|, \frac{|C_G(x):C_H(x)|}{|N_G(x):H|} \right)$$

design constructed by Theorem 3.2. If $T = \bigcup_{i=1}^m x_i^H$ is a partition of all $\{x_i^H : x_i \in G\}$, where $x_i^H \cap x_j^H = \emptyset$ for $1 \leq i, j \leq m$, then we can construct a

$$1 - \left(|x^G|, |T|, \sum_{i=1}^m \frac{|C_G(x):C_H(x_i)|}{|N_G(T):H|} \right)$$

design.

Proof The proof follows by Theorem 3.2 and Proposition 3.5. $\square$

Corollary 3.7 (Key–Moore Method 2) Let G be a finite simple group, M a maximal subgroup of G and x^G a conjugacy class of elements of order n in G such that

$$M \cap x^G \neq \emptyset.$$

Then we have a $1 - (|x^G|, |M \cap x^G|, \chi_M(x))$ design $\mathcal{D}$. The group G acts as an automorphism group on $\mathcal{D}$, primitive on blocks and transitive on points of $\mathcal{D}$.

Proof It suffices to notice that $T = M \cap x^G$ is a union of some conjugacy classes of G . Now by Proposition 3.6, we can construct a

$$1 - \left(|x^G|, |T|, \sum_{i=1}^m \frac{|C_G(x):C_H(x_i)|}{|N_G(T):M|} \right)$$

design. Moreover, maximality of M implies that $N_G(M) = N_G(T) = M$. So we have:

$$\lambda = \frac{|M|}{|N_G(T)|} \times \sum_{i=1}^m \frac{|C_G(x)|}{|C_H(x_i)|} = \frac{|M|}{|N_G(M)|} \times \sum_{i=1}^m \frac{|C_G(x)|}{|C_H(x_i)|} = \chi_M(x),$$

rendering to be a corollary to Proposition 3.6. $\square$

In what follows, we apply the method outlined in Theorem 3.2 to investigate designs invariant under the groups J_1 and $PSL_2(q)$, where q is a power of 2. We begin by computing the designs for J_1 across all its maximal subgroups, which allows us to identify additional designs that cannot be obtained by Method 2. Next, we classify the designs constructed by three non-maximal subgroups of $PSL_2(q)$.

4 Designs and codes from sporadic simple groups

In this section, we apply our method to construct 1-designs and binary linear codes from the maximal subgroups and conjugacy classes of some sporadic simple groups. We use MAGMA [2] for the computations. Due to computational limitations, we are not able to find all possible codes and their properties; however, our search has led to the discovery of codes with interesting parameters. We note that most of the designs constructed using our method have strength one. Nevertheless, we have found a few examples that satisfy the conditions for 2-designs. For instance, using the symmetric group S_6 and the class of fixed-point-free involutions, we obtained a 2-(15, 8, 4) design. For the symplectic group $PSp_4(3)$, we constructed 2-(40, 12, 3) and 2-(40, 27, 18) designs. Also, some 2-(63, 32, 16) designs can be constructed from the unitary group $U(3, 3)$. However, such cases are rare, and in general, the resulting designs appear to be 1-designs.

We begin with the Janko group J_1 , a simple group of order 175560 and one of the 26 sporadic simple groups. It can be characterized abstractly as the unique simple group with abelian 2-Sylow subgroups and an involution whose centralizer is isomorphic to the direct product of a group of order two and the alternating group A_5 . Moreover, J_1 has 15 conjugacy classes. Here we apply our method to the Janko group $G = J_1$ to construct 1-designs invariant under G . For detailed information on this group, see [6].

We focus on a maximal subgroup of index 2926. The complete list of designs constructed using this method, which are invariant under J_1 (as well as some other small sporadic simple groups), is provided in [28]. A maximal subgroup of G with index 2926 is isomorphic to $D_6 \times D_{10}$ (Table 1). The parameters of the 1-designs corresponding the conjugacy classes of G which are constructed by our method are given in Table 3.

The designs constructed using Key–Moore Method 2 are as follows:

$$1\text{--}(5852, 2, 1), 1\text{--}(17556, 6, 1), 1\text{--}(11704, 4, 1), 1\text{--}(29260, 10, 1), 1\text{--}(1463, 23, 46).$$

The first four designs have been also derived by our method and appeared in Table 3. However, we can see that the design with parameters $1 - (1463, 23, 46)$ has not appeared in the table. Therefore, it should result from a merge of some designs listed in it. Specifically, we can see that merging the following three 1-designs, which have been bolded in the table:

$$1 - (1463, 3, 6), \quad 1 - (1463, 5, 10), \quad 1 - (1463, 15, 30)$$

will produce a $1 - (1463, 23, 46)$ design. Here we construct a code from a $1\text{--}(1463, 3, 6)$ design.

Now we assume that C is the dual of the binary linear code generated by a $1\text{--}(1463, 3, 6)$ design D constructed using the method presented in this paper. This code has parameters $[1463, 20, 608]$ and has been mentioned by Moore in [13, Page 20]. Although the code has

Table 1 The designs by J_1 , where H is the maximal subgroup of G with index 2926

Conjugacy classes $Cl(i)$	Designs $1 - (v, k, \lambda)$		
$Cl(2)$	$1 - (1463, 3, 6)$ $1 - (1463, 30, 60)$	$1 - (1463, 5, 10)$ $1 - (1463, 60, 120)$	$1 - (1463, 15, 30)$
$Cl(3), Cl(4), Cl(5)$	$1 - (5852, 2, 1)$	$1 - (5852, 30, 15)$	$1 - (5852, 60, 30)$
$Cl(6)$	$1 - (29260, 10, 1)$	$1 - (29260, 30, 3)$	$1 - (29260, 60, 6)$
$Cl(7)$	$1 - (25080, 60, 7)$		
$Cl(8), Cl(9)$	$1 - (17556, 6, 1)$	$1 - (17556, 30, 5)$	$1 - (17556, 60, 10)$
$Cl(10)$	$1 - (15960, 60, 11)$		
$Cl(11), Cl(12)$	$1 - (11704, 4, 1)$	$1 - (11704, 60, 15)$	
$Cl(13), Cl(14), Cl(15)$	$1 - (9240, 60, 19)$		

already been noted in previous work, its parameters remain of considerable interest, and further investigation into its properties could prove valuable.

The following results are based on MAGMA and provide more detailed information on the structure of this code.

- (i) C is an irreducible doubly even (and hence self-orthogonal) code. Notice that the irreducibility of C follows from the fact that 20 is the smallest degree of a non-trivial irreducible module of J_1 .
- (ii) We have $Aut(D) = Aut(C) = J_1$.
- (iii) The weight distribution of C is given as follows.

$$0^1, 608^{1540}, 632^{2926}, 640^{7315}, 688^{29260}, 696^{29260}, 712^{87780}, 720^{89243}, \\ 728^{311410}, 736^{87780}, 744^{175560}, 752^{222376}, 760^{3080}, 784^{1045}$$

- (iv) The stabilisers of the codewords of C are given at the Table 2. Notice that in Table 2, F_{42} , F_{114} , and F_{168} are Frobenius groups of types 7:6, 19:6 and $2^3:7:3$ respectively, and are all maximal subgroups of J_1 .
- (v) The code $C \oplus C_1$ where C_1 is the repetition code of length 1463 has parameters $[1463, 21, 608]$.

Some other sporadic simple groups

We searched for binary linear codes with interesting parameters that can be constructed using our method. While some of these codes may already be known, our goal was not to verify their novelty or to conduct a detailed analysis of their properties. Rather, we present in Table 3, a selection of examples, listing only their parameters and the simple groups from which they are derived. Readers who find the parameters interesting may further investigate the codes and their properties.

Table 2 The stabilisers of the codewords of $\mathcal{C} = [1463, 20, 608]_2$

Weight	#Orb	Stab	Size	Is maximal
608	1	F_{114}	1540	Yes
632	1	A_5	2926	No
640	1	$A_4 \times C_2$	7315	No
688	1	S_3	29260	No
696	2	D_{12}	14630, 14630	No
712	1	C_2	87780	No
720	2	$C_2 \times A_5, C_2$	1463, 87780	Yes, No
728	7	$F_{42}, D_{12}, S_3, S_3,$ C_3, C_2, C_2	4180, 14630, 29260, 29260, 58520, 87780, 87780	Yes, No, No, No, No, No, No
736	2	S_3, C_3	29260, 58520	No
744	2	C_2, C_2	87780, 87780	No
752	6	$C_{10}, C_6, S_3, C_6,$ C_3, C_3	17556, 29260, 29260, 29260, 58520, 58520	No
760	1	C_{57}	3080	No
784	1	F_{168}	1045	Yes

Table 3 Some codes with interesting parameters

Group	Parameters of the binary codes invariant under the group
M_{11}	[1584, 22, 264] – [165, 54, 20] – [440, 65, 36] – [990, 153, 32]
M_{12}	[495, 11, 234] – [990, 21, 288] – [440, 22, 80] – [396, 44, 96]
M_{23}	[1680, 11, 3795] – [1155, 12, 3795] – [1320, 22, 3795]
J_1	[1463, 20, 608]
J_2	[560, 14, 260] – [315, 36, 80]

5 Some designs under the projective linear group

In this section, we apply the method described in Theorem 3.2 to find the parameters of designs invariant under the projective linear group $PSL_2(q)$, where q is a power of 2. The case where q is odd will be addressed in our forthcoming paper [25].

Let $G = PSL_2(q)$, where q is a power of 2. We assume that the reader is familiar with the basic structure of G . However, for the readers convenience, we restate some well-known results that we have used in this paper. For more detailed information on these groups, one can refer to [9, 29]. The order of G equals $(q-1)q(q+1)$. Let S be a subgroup of G of order $s \in \{q \pm 1, q\}$. Then, for all $x \in S$, we have $S = C_G(x)$. Also, $S \cap S^g = 1$ or S , for all $g \in G$, and every subgroup of order s in G is conjugate to S . The normalizer of S in G is a maximal subgroup of G . If $s = q$, then $N_G(S)$ is a Frobenius group of order $q(q-1)$. In this case, S is the Frobenius kernel of $N_G(S)$. Notice that in this case, S is a Sylow 2-subgroup of G , which is elementary abelian. Moreover, G contains exactly one class of involutions. Now assume that $s = q \pm 1$. Then $N_G(S)$ is a dihedral group of order $2|S|$. So we have three classes of maximal subgroups of G that appear for all values of q . For some values of q , we may have maximal subgroups of type $PSL_2(q_0)$, where q_0 divides q . Some designs under

the projective linear group G have been achieved using Key–Moore Methods [21]. Now, we aim to construct some additional designs under the group G using Theorem 3.2.

Proposition 5.1 [7] *Let G be a Frobenius group with kernel N and let K be a subgroup of G . Then one of the following must occur:*

1. $K \subseteq N$.
2. $K \cap N = \{1_G\}$.
3. K is a Frobenius group with kernel $K \cap N$.

Proposition 5.2 [5] *Suppose that G is a Frobenius group with complement H and kernel N . Then $o(H) \mid o(N) - 1$.*

Lemma 5.3 *Let S be a subgroup of G and x is an element of G , where $x \notin S$. If $N_G(S) \cap C_G(x) = 1$, then $N_G(x^S) = S$.*

Proof By Lemma 3.1 we have

$$N_G(x^S) = N_G(x^S) \cap C_G(x)S = (N_G(x^S) \cap C_G(x))S = S.$$

□

Theorem 5.4 *Let $G = PSL_2(q)$, where q is a power of 2. Assume that*

$$s, s' \in \{q \pm 1, q\}.$$

Suppose that S is a subgroup of G of order s and x is an element of G such that $o(x)$ divides s' . Then we can construct the designs with the following parameters in different cases:

1. If $(s, s') \notin \{(q \pm 1, q), (q, q - 1)\}$, then we have a $1 - \left(\frac{|G|}{s'}, s, s'\right)$ design.
2. If $s = q + 1$ and $s' = q$, then we have a $1 - \left(\frac{|G|}{s'}, s, \frac{s'}{2}\right)$ design.
3. If $s = q$ and $s' = q - 1$,
 - (a) If $N_G(S) \cap C_G(x) \neq 1$, then we have a $1 - \left(\frac{|G|}{s'}, s, 1\right)$.
 - (b) If $N_G(S) \cap C_G(x) = 1$, then we have a $1 - \left(\frac{|G|}{s'}, s, s'\right)$.
4. If $s = q - 1$ and $s' = q$, then we have a $1 - \left(\frac{|G|}{s'}, s, 1\right)$ or a $1 - \left(\frac{|G|}{s'}, s, \frac{s'}{2}\right)$ design.

Proof According to the properties of $PSL_2(q)$, we have $|C_G(x)| = s'$. Therefore in all cases we have $v = |x^G| = \frac{|G|}{s'}$. On the other hand, the size of each block is

$$k = |x^S| = \frac{|S|}{|S \cap C_G(x)|} = s.$$

To complete the proof, we only need to find the third parameter of the designs in each case. Note that in all cases

$$\lambda = \frac{kb}{v} = \frac{ss'|G|}{|N_G(x^S)||G|} = \frac{ss'}{|N_G(x^S)|}.$$

Therefore, $|N_G(x^S)|$ divides ss' . Also, s divides $|N_G(x^S)|$, since $S \leq N_G(x^S)$.

The subgroup $N_G(x^S)$ is contained in some maximal subgroups of G of orders $2(q-1)$, $2(q+1)$ or $q(q-1)$. Notice that G may also have a maximal subgroup of order $q_0(q_0-1)(q_0+1)$ (where q_0 divides q), however, $N_G(x^S)$ is not contained in this maximal subgroup, since it contains S . Now we consider the following steps and find $|N_G(x^S)|$ in each case. The third parameter can be obtained using the size of $N_G(x^S)$.

Step 1: If $s = q$, and $s' \neq q-1$, then $|N_G(x^S)| = q$. Since $|S| = q$ divides $|N_G(x^S)|$, then $N_G(x^S)$ lies in a maximal subgroup of order $q(q-1)$. On the other hand, $|N_G(x^S)|$ divides $ss' = q^2$ or $q(q+1)$. Since $q-1$ is relatively prime to both q and $q+1$, we conclude that $|N_G(x^S)| = q$.

Step 2: If $s = q$, and $s' = q-1$, then $|N_G(x^S)| = q$ or $|N_G(x^S)| = q(q-1)$. We have q divides $|N_G(x^S)|$, and $|N_G(x^S)|$ divides $q(q-1)$. So $N_G(x^S)$ must be a subgroup of the maximal subgroup F of order $q(q-1)$, which is a Frobenius group with kernel S . Let $F = SH$, where H is a Frobenius complement of H . Now we consider the following cases:

- (a) If $N_G(S) \cap C_G(x) = 1$, then by Lemma 5.3, $N_G(x^S) = S$. Therefore, $|N_G(x^S)| = q$.
- (b) If $F \cap C_G(x) \neq 1$, then by the properties of the Frobenius groups [5], $C_G(x)$ non-trivially intersects one of the complements of F . Hence, $C_G(x)$ must be a Frobenius complement of F . Therefore,

$$N_G(S) \cap C_G(x) = F \cap C_G(x) = C_G(x),$$

and using Lemma 3.1, we obtain $|N_G(x^S)| = q(q-1)$.

Step 3: If $s = q+1$, and $s' \neq q$, then $|N_G(x^S)| = q$.

Since $q+1$ divides $|N_G(x^S)|$ and x is not an involution, we deduce that $N_G(x^S)$ lies in a maximal subgroup of order $2(q+1)$. On the other hand, $|N_G(x^S)|$ divides either $(q+1)^2$ or q^2-1 . In any case, we must have $|N_G(x^S)| = q+1$.

Step 4: If $s = q+1$, and $s' = q$, then $|N_G(x^S)| = 2(q+1)$.

A similar argument to the one used in the previous steps shows that $N_G(x^S)$ lies in a maximal subgroup of order $2(q+1)$. Therefore, $|N_G(x^S)| = q+1$ or $2(q+1)$. We claim that the former does not occur. Notice that $N_G(S)$ is a Frobenius group with exactly $q+1$ involutions. Also $C_G(x)$ has exactly $q+1$ conjugates in G . This implies that $C_G(x)$ contains one of the involutions of $N_G(S)$. In particular, $|N_G(S) \cap C_G(x)|$ is even. So by Lemma 3.1, $|N_G(x^S)| = 2(q+1)$.

Step 5: If $s = q-1$, and $s' \neq q$, then $|N_G(x^S)| = q-1$. The result follows, using a similar argument to Step 3.

Step 6: If $s = q-1$, and $s' = q$, then $|N_G(x^S)| = 2(q-1)$ or $q(q-1)$.

In this case, $q-1$ divides $|N_G(x^S)|$, and $|N_G(x^S)|$ divides $q(q-1)$. So $N_G(x^S)$ must be a subgroup of a maximal subgroup of order $2(q-1)$ or $q(q-1)$.

- (a) If $N_G(x^S)$ lies in a maximal subgroup of order $2(q-1)$, then $|N_G(x^S)| = q-1$ or $2(q-1)$. Using a similar argument to Step 4, products $|N_G(x^S)| = 2(q-1)$.
- (b) If $N_G(x^S)$ is a subgroup of a Frobenius group $F = NS$ of order $q(q-1)$, where N is the Frobenius kernel of order q , and S is a Frobenius complement, then by Proposition 5.1, we must have $N_G(x^S) \leq N$, $N_G(x^S) \cap N = 1$ or $N_G(x^S)$ is a Frobenius group. It is clear that the first condition fails. We claim that $N_G(x^S) \cap N \neq 1$. Assume to the contrary that $N_G(x^S) \cap N = 1$. Then $N_G(x^N)$ is a Frobenius complement of F . In particular, $|N_G(x^S)| = q-1$. On the other hand, a similar argument to Step 4 implies that $N_G(S) \cap C_G(x)$ contains an involution. Therefore

Table 4 Designs from $G = PSL_2(q)$, where q is a power of 2

s'	s		
	$q - 1$	q	$q + 1$
$q - 1$	$1 - (q^2 + q, q - 1, q - 1)$	$1 - (q^2 + q, q, q - 1)$ $1 - (q^2 + q, q, 1)$	$1 - (q^2 + q, q + 1, q - 1)$
q	$1 - (q^2 - 1, q - 1, \frac{q}{2})$ $1 - (q^2 - 1, q - 1, 1)$	$1 - (q^2 - 1, q, q)$	$1 - (q^2 - 1, q + 1, \frac{q}{2})$
$q + 1$	$1 - (q^2 - q, q - 1, q + 1)$	$1 - (q^2 - q, q, q + 1)$	$1 - (q^2 - q, q + 1, q + 1)$

by Lemma 3.1, $N_G(x^S)$ contains an involution which is a contradiction. This proves the claim. In particular, $N_G(x^S)$ must be a Frobenius group with kernel $N \cap N_G(x^S)$. If $N \cap N_G(x^S) \neq N$, then we reach a contradiction using Proposition 5.2. Hence, $N_G(x^S) = N$ and we have $|N_G(x^S)| = q(q - 1)$.

□

Remark 2 Except for the $1 - (q^2 - 1, q - 1, 1)$ and $1 - (q^2 - 1, q \pm 1, \frac{q}{2})$ designs, which were constructed using the Key–Moore method 2 (see [21]), the remaining 1-designs in Theorem 5.4 are new. The results of Theorem 5.4 are summarised in Table 4.

Acknowledgements The authors thank both reviewers for their valuable comments and suggestions. They also acknowledge the Centre for High Performance Computing (CHPC), South Africa, for providing the computational resources used in this research project.

Author Contributions All authors reviewed the manuscript and contributed equally to this work.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no Conflict of interest.

References

- Assmus E.F., Key J.D.: Designs and Their Codes, vol. 103. Cambridge University Press (Cambridge Tracts in Mathematics), Cambridge (1992)
- Bosma W., Cannon J., Playoust C.: The Magma algebra system. I: The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997).
- Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A.: Atlas of Finite Groups. Oxford Univ. Press, Oxford (1985)
- Crnković D., Crnković V.M., Švob A.: On some transitive combinatorial structures constructed from the unitary group $U(3,3)$. J. Stat. Plann. Inference **144**, 19–40 (2014).
- Flavell P.: A note on Frobenius groups. J. Algebra **228**(1), 367–376 (2000).
- Janko Z.: A new finite simple group with abelian sylow subgroups and its characterization. J. Algebra **3**, 147–186 (1966).
- Karpilovsky, G.: Group Representations Volume 1, Part A: Background Material. Elsevier Science Publishers B.V., The Netherlands (1992)
- Key J.D., Moore J.: Designs, codes and graphs from the janko groups J_1 and J_2 . J. Comb. Math. Comb. Comput. **40**, 143–159 (2002).

9. King O.H.: The subgroup structure of finite classical groups in terms of geometric configurations, surveys in combinatorics. London Mathematical Society Lecture Note Series, Cambridge: Cambridge University Press **327**, 29–56 (2005).
10. Mbaale X., Rodrigues B.G.: Symmetric 1-designs from $PSL_2(q)$, for q a power of an odd prime. Trans. Comb. **10**(1), 43–61 (2021).
11. Mbaale X., Rodrigues B.G.: Symmetric 1-designs from $PGL_2(q)$, for q an odd prime power. Glas. Mat. Ser. III **56**(76), 1–15 (2021).
12. Mbaale X., Rodrigues B.G., Zandi S.: Designs from maximal subgroups and conjugacy classes of $PSL(2, q)$, q odd. AUT J. Math. Comput. **4**(1), 47–55 (2023).
13. Moori J.: Finite groups, designs and codes. Information Security, Coding Theory and Related Combinatorics, Nato Science for Peace and Security Series D: Information and Communication Security **29**, 202–230 (2011).
14. Moori J.: Designs and codes from fixed points of finite groups. Commun. Alg. **49**(2), 706–720 (2021).
15. Moori J.: Designs and codes from involutions of A_n . Quaest. Math. **45**(6), 1–15 (2021).
16. Moori J.: Designs and codes from basic 3-transpositions. Bull. Iran. Math. Soc. **48**(5), 2855–2871 (2022).
17. Moori J., Rodrigues B.G.: A self-orthogonal doubly even code invariant under $M^cL:2$. J. Comb. Theory Ser. A. **110**(1), 53–69 (2005).
18. Moori J., Rodrigues B.G.: Some designs and codes invariant under the simple group Co_2 . J. Algebra **316**(2), 649–661 (2007).
19. Moori J., Rodrigues B.G.: On some designs and codes invariant under the Higman–Sims group. Util. Math. **86**, 225–239 (2011).
20. Moori J., Saeidi A.: Some designs and codes invariant under the Tits group. Adv. Math. Commun. **11**(1), 77–82 (2017).
21. Moori J., Saeidi A.: Constructing some designs invariant under $PSL_2(q)$, q even. Commun. Alg. **46**(1), 160–166 (2018).
22. Moori J., Saeidi A.: Some designs and codes invariant under the Suzuki group. Util. Math. **109**, 105–114 (2018).
23. Moori J., Rodrigues B.G., Saeidi A., Zandi S.: Some symmetric designs invariant under the small Ree groups. Commun. Alg. **47**(5), 2131–2148 (2019).
24. Moori J., Rodrigues B.G., Saeidi A., Zandi S.: Designs from maximal subgroups and conjugacy classes of Ree groups. Adv. Math. Commun. **14**(4), 603–611 (2020).
25. Saeidi, A., Saydi, H.: Some new designs under $PSL_2(q)$, q odd (under preparation)
26. Saeidi A.: Designs and codes from fixed points of alternating groups. Commun. Alg. **50**(5), 2215–2222 (2022).
27. Saeidi A.: Reduced designs constructed by Key–Moori Method 2 and their connection with method 3. AUT J. Math. Comput. **4**(1), 39–46 (2023).
28. Saeidi A.: Designs invariant under simple groups: magma computations. Zenodo (2024). <https://doi.org/10.5281/zenodo.13854113>.
29. Wilson R.A.: The Finite Simple Groups. Springer, London (2009).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.